IN THE CLAIMS:

Claims 39 and 42 have been cancelled. Claims 30, 33, 38, and 41 have been amended, as follows:

Claims 1 - 28 (cancelled).

29. (previously presented) A method of generating a private encryption key, comprising:

generating a public encryption key and a private encryption key at a client system;

inputting a password and generating a random number;

creating a random private key by exclusive-ORing the private key with the random number;

generating a first hash value by hashing the password, a username, and a constant value;

encrypting the random private key using the first hash value as an encryption key to create an encrypted random key;

generating a second hash value by hashing the password, the username, and a second constant value; and

transmitting the username, the second hash value, and the encrypted random key to a server for storage.

30. (currently amended) The method of claim 29, further including further

authenticating a user at the [[remote]] server.

31. (previously presented) The method of claim 30, wherein the method of authenticating is using a biometric device.

32. (previously presented) The method of claim 29, further including deleting the private encryption key from the client system.

33. (currently amended) The method of claim 29, further including deleting the [[first]] constant value from the client system.

34. (previously presented) A computer readable medium containing instructions for execution by a processor, the instructions, which when executed, cause the processor to:

generate a public encryption key and a private encryption key at a client system, which includes the processor;

receive a password and generate a random number;

create a random private key by exclusive-ORing the private key with the random number;

generate a first hash value by hashing the password, a username, and a constant value;

encrypt the random private key using the first hash value as an encryption key to create an encrypted random key;

generate a second hash value by hashing the password, the username, and a second constant value; and

transmit the username, the second hash value, and the encrypted random key to a server for storage.

35. (previously presented) The computer-readable medium of claim 34, including instructions, which when executed causes the processor to delete the private encryption key from the client system.

36. (previously presented) The computer-readable medium of claim 34, including instructions, which when executed causes the processor to delete the constant value.

37. (previously presented) The computer-readable medium of claim 34, including instructions, which when executed causes the processor to delete the second constant value.

38. (currently amended) A method for retrieving a stored password, comprising:

receiving a password and a username;

generating a first hash value using the password, the username, and a first constant value;

generating a second hash value using the password, the username, and a second constant value;

transmitting the second hash value and the username to a key server; [[and]]

receiving an encrypted random private key from the key server if the username and the second hash value match a stored username value and a stored hash value; and

decrypting the encrypted random private key using the first has value as an encryption key to generating a random private key.

Claim 39 (cancelled).

40. (previously presented) The method of claim 38, further including exclusive-ORing a random number with the random private key to generate a private key.

41. (currently amended) A computer readable medium containing instructions for execution by a processor, the instructions, which when executed, cause the processor to:

receive a password and a username;

generate a first hash value using the password, the username, and a first constant value;

generate a second hash value using the password, the username, and a second constant value;

transmit the second hash value and the username to a key server; [[and]]

receive an encrypted random private key from the key server if the username and the second hash value match a stored username value and a stored hash value; and

decrypt the encrypted random private key using the first hash value as an encryption key to generate a random private key.

Claim 42 (cancelled).

43. (previously presented) The computer-readable medium of claim 41, including instructions, which when executed causes the processor to exclusive-OR a random number with the random private key to generate a private key.